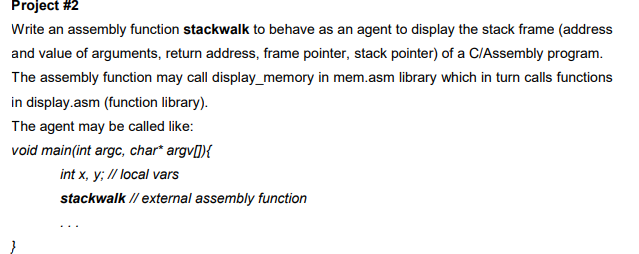
Project #2



Write an assembly function stackwalk to behave as an agent to display the stack frame (address and value of arguments, return address, frame pointer, stack pointer) of a C/Assembly program. The assembly function may call display\_memory in mem.asm library which in turn calls functions in display.asm (function library). The agent may be called like: void main(int argc, char\* argv[]){ int x, y; // local vars stackwalk // external assembly function . . . }

Submission:

You are required to submit a RAR file that includes:

- Source code of the tasks including full comments (file .asm)

- A comprehensive report of how you develop your code, use the libraries, test your code and how you overcome the difficulties. (file .docx) The RAR file must be named in this convention: For example: Lê Thiện An, 19110105 will submit the file as 19110105\_LeThienAn.RAR

Grading:

- Program works as in the project statement: 5 (pts)

- Bonus for an outstanding solution and beautiful code (1.5 pts)

- Thorough and Comprehensive report (2.5 pts)

- Well-formatted report (1 pts)

sẽ in ra stack frame của 1 chương trình, lấy đúng vị trí của các thành phần trong stack frame để in ra (hàm stackwalk hoạt động như 1 nhân tố agent)

stackframe gồm ( địa chỉ tham số, địa chỉ trả về,...)

cho biết biến x,y địa chỉ, giá trị là bao nhiêu từ esp tính được tất cả các địa chỉ từ y-> argv.

Vấn đề: xác định đúng vị trí của các thành phần trên stackframe, xử dụng các hàm writehex,writehexdigit,writehexword hoặc writehexdword mà 32 bit nên làm trên write

https://wiki.osdev.org/Stack\_Trace

Find a way to print the stackframe of a function call. Test in various cases : Program c that calls assembly functions in one level and multiple-level ?

+ Find a way to print the stack frame of a function call.

+ Test it in various cases: A C program that calls assembly functions in one-level or multiple-level.

As I understand you need to print passed parameters. Here's the code below for printing two parameters.

Read also [https://stackoverflow.com/.../what-is-stack-frame-in...](https://stackoverflow.com/questions/3699283/what-is-stack-frame-in-assembly)

myfunction( 'a','b');

myfunction:

push bp

mov bp,sp

mov al, [bp+4] ;first parameter 'a'

mov ah,0eh ;print character

int 10h

mov al, [bp+5] ;second parameter 'b'

mov ah,0eh ;print character

int 10h

And this to read about stack <https://www.csee.umbc.edu/~chang/cs313.s02/stack.shtml>

<https://manybutfinite.com/post/journey-to-the-stack/>